441 G St. N.W.
Washington, DC 20548

Accessible Version

January 28, 2021

The Honorable Gregory W. Meeks
Chairman
The Honorable Michael T. McCaul
Ranking Member
Committee on Foreign Affairs
House of Representatives

CYBER DIPLOMACY: State Should Use Data and Evidence to Justify Its Proposal for a New Bureau of Cyberspace Security and Emerging Technologies

The United States and its allies are facing expanding foreign cyber threats, as international trade, communication, and critical infrastructure become increasingly dependent on cyberspace. The United States also faces challenges to build consensus within international organizations on setting standards for how to govern the internet and cultivating norms for acceptable government behavior in cyberspace.

The Department of State (State) leads U.S. government international efforts to advance the full range of U.S. interests in cyberspace. In January 2019, members of Congress introduced the Cyber Diplomacy Act of 2019,[1] which would have established a new office to lead State's international cyberspace efforts that would consolidate cross-cutting efforts on international cybersecurity, digital economy, and internet freedom, among other cyber diplomacy issues.[2]

In June 2019, State notified Congress of its intent to establish a new Bureau of Cyberspace Security and Emerging Technologies (CSET). In contrast to the proposed legislation discussed above, State intended that its new bureau would focus more narrowly on cyberspace security and the security aspects of emerging technologies.[3] According to State officials, Members of Congress raised objections to State's plan. On January 7, 2021, State announced that the

[1]*Cyber Diplomacy Act of 2019*, H.R. 739, 116th Cong. (2019). The House Foreign Affairs Committee reported out this bill, co-sponsored by 29 members of Congress, by voice vote in March 2019, but the full House of Representatives did not consider the bill prior to expiration of the 116th Congress. The House of Representatives passed a similar version of the bill during the 115th Congress, *Cyber Diplomacy Act of 2017*, H.R. 3776, 115th Cong. (2017).

[2]According to State, the term "cyber diplomacy" encompasses a wide range of U.S. interests in cyberspace. These include cybercrime, cybersecurity, digital economy, international development and capacity building, internet freedom, and internet governance. Others have defined cyber diplomacy as diplomacy in a cyberspace environment, in particular for building strategic international partnerships to support national interests. See A. Barrinha and T. Renard, "Cyber-diplomacy: the making of an international society in the digital age," *Global Affairs*, vol. 3, no. 4-5 (2017); and C. Painter, "Diplomacy in Cyberspace," *The Foreign Service Journal*, vol. 95, no. 5 (2018).

[3]In March 2020, the Cyberspace Solarium Commission recommended, among other things, the creation of a CSET bureau at State, which would report to the Under Secretary of Political Affairs or someone of higher rank. Accessed March 11, 2020. https://www.solarium.gov/report. In July 2020, the National Security Commission on Artificial Intelligence recommended to create a CSET bureau reporting to the Under Secretary for Arms Control and International Security. Accessed September 10, 2020. https://www.nscai.gov/.

Secretary had approved the creation of CSET and directed the department to move forward with establishing the bureau. However, as of the date of this report, State had not created CSET.

We reported in September 2020 that State did not involve federal agency partners in its plan to establish CSET. In the report, we recommended State involve federal agencies that contribute to cyber diplomacy to obtain their views and identify any risks, such as unnecessary fragmentation, overlap, and duplication of efforts, as it implements its plan to establish CSET.[4] State did not agree with our recommendation, noting that it was unaware that these agencies had consulted with State before reorganizing their own cyberspace security capabilities and organizations. We stand by the recommendation and maintain that it is important for State, as the leader of U.S. government international efforts to advance U.S. interests in cyberspace, to incorporate leading practices to ensure the successful implementation of its reorganization effort and to reduce the potential for any unwarranted overlap and duplication in its efforts.

You asked us to review State's efforts to advance U.S. interests in cyberspace.[5] This report examines the extent to which State used data and evidence to develop and justify its proposal to establish CSET.

To address this objective, we interviewed State officials and reviewed documentation from State on its planning process for establishing the new bureau. We assessed State's documentation against the key practice of using data and evidence in the development of the proposed agency reforms, drawn from our June 2018 report on government reorganization.[6] To address this practice, we analyzed State's activities leading to the development of the June 2019 Congressional Notification on its proposal for establishing CSET. We also consulted our prior work on agencies' efforts to develop and use evidence to support their decision-making, which highlights decision makers' need for using evidence to help address pressing governance challenges faced by the federal government.[7]

We conducted this performance audit from July 2019 to January 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[4]GAO, *Cyber Diplomacy: State Has Not Involved Relevant Federal Agencies in the Development of Its Plan to Establish the Cyberspace Security and Emerging Technologies Bureau*, GAO-20-607R (Washington, D.C.: Sep. 22, 2020).

[5]We initiated this work at the request of Representative Eliot L. Engel, Chairman, and Representative Michael T. McCaul, Ranking Member, of the House Committee on Foreign Affairs of the 116th Congress.

[6]GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, GAO-18-427 (Washington, D.C.: June 13, 2018).

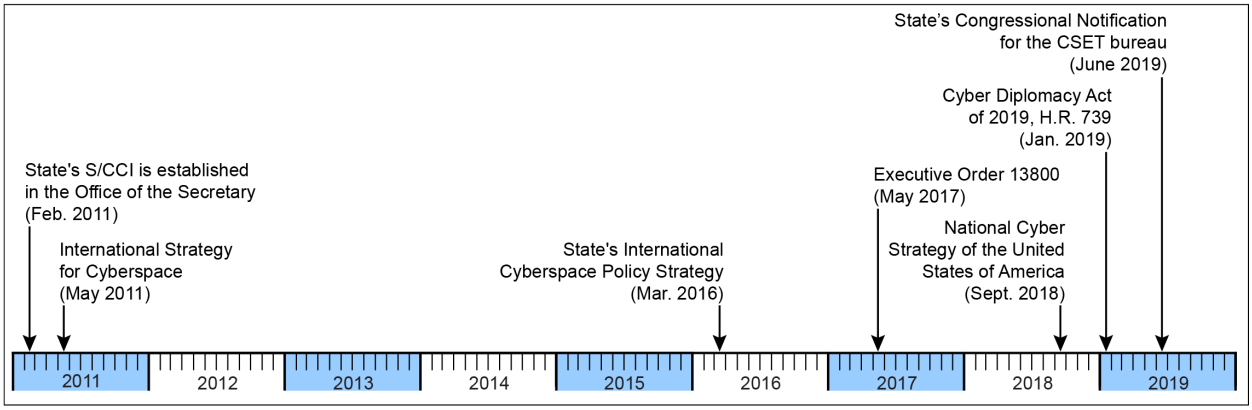
[7]GAO, *Evidence-Based Policymaking: Selected Agencies Coordinate Activities, but Could Enhance Collaboration*, GAO-20-119 (Washington, D.C.: Dec. 4, 2019).

Background

State's Role in U.S. Cyber Diplomacy

Since 2011, the United States has recognized the importance of international cyber diplomacy, and State has taken a lead role in carrying out U.S. cyber diplomacy objectives. Figure 1 provides a timeline of key strategies and events in State's involvement in cyber diplomacy.

Figure 1: Timeline of Key Strategies and Events in the Department of State's Involvement in Cyber Diplomacy



Legend: Cyberspace Security and Emerging Technologies = CSET; Department of State = State; Office of the Coordinator for Cyber Issues = S/CCI.

Source: GAO analysis of agency documents. | GAO-21-266R

Text of Figure 1: Timeline of Key Strategies and Events in the Department of State's Involvement in Cyber Diplomacy

1. State's S/CCI is established in the Office of the Secretary (Feb. 2011)
2. International Strategy for Cyberspace (May 2011)
3. State's International Cyberspace Policy Strategy (Mar. 2016)
4. Executive Order 13800 (May 2017)
5. National Cyber Strategy of the United States of America (Sept. 2018)
6. Cyber Diplomacy Act of 2019, H.R. 739 (Jan. 2019)
7. State's Congressional Notification for the CSET bureau (June 2019)

Source: GAO analysis of agency documents. | GAO-21-266R

- In February 2011, State established the Office of the Coordinator for Cyber Issues (S/CCI) in the Office of the Secretary to lead the department's global diplomatic engagement on cyber issues and to serve as liaison to other federal agencies that work on cyber issues.

- In May 2011, the White House issued the *International Strategy for Cyberspace*,[8] which called for strengthening partnerships with other countries to build consensus around principles of responsible behavior in cyberspace. This strategy included the goal to work

[8]The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, D.C.: May 16, 2011).

with the international community to promote an open, interoperable, secure, and reliable information and communications infrastructure.[9]

- In March 2016, State issued the *International Cyberspace Policy Strategy* report to Congress, as mandated by the Cybersecurity Act of 2015,[10] which affirmed the elevation of cyberspace policy as a foreign policy imperative and the prioritization of its efforts to mainstream cyberspace policy issues within the department's diplomatic activities.

- In May 2017, the White House issued Executive Order 13800, which required, among other things, that the Secretary of State coordinate with other agencies to submit reports to the President on (1) options for deterring adversaries and protecting the United States from cyber threats, and (2) an engagement strategy for international cooperation on cybersecurity.[11]

- In September 2018, the White House issued the *National Cyber Strategy of the United States of America,*[12] which renewed the commitment to expand American influence abroad to protect and promote an open, interoperable, reliable, and secure internet, as one of its 10 objectives.

- In January 2019, members of Congress introduced the Cyber Diplomacy Act of 2019.

Building Evidence into Reform Efforts

Successful reforms require an integrated approach built on the use of data and evidence.[13] Such an approach is critical for setting program priorities, allocating resources, and taking corrective action to solve performance problems and improve results.[14] Our prior work has shown that federal decision makers need evidence about whether federal programs and activities achieve intended results as they set priorities and consider how to make progress toward objectives.[15] In addition, we have reported that agencies are better able to address management and performance challenges when managers effectively use data and evidence to achieve program goals. Agencies can also use data and evidence when reforming programs to

[9]The strategy defined four key characteristics of cyberspace: (1) open to digital innovation; (2) interoperable around the world; (3) secure enough to maintain users' trust; and (4) reliable enough to support their work.

[10]Pub. L. No. 114-113, Div. N, § 402.

[11]State released summaries of these two reports in May 2018. According to State officials, State developed these reports in coordination with other executive branch agencies. The first report recommended an approach for imposing consequences on foreign governments responsible for significant malicious cyber activities aimed at harming U.S. national interests. The second report established a set of objectives and associated actions for cyberspace policy to achieve an open, interoperable, reliable, and secure internet.

[12]The White House, *National Cyber Strategy of the United States of America* (Washington, D.C.: Sept. 20, 2018).

[13]For purposes of this report, we use the definition of evidence contained in OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, pt. 6, §200.22 (July 2020), which describes evidence as the available body of facts or information indicating whether a belief or proposition is true or valid.

[14]GAO, *Managing for Results: Further Progress Made in Implementing the GPRA Modernization Act, but Additional Actions Needed to Address Pressing Governance Challenges*, GAO-17-775 (Washington, D.C.: Sep. 29, 2017).

[15]GAO-20-119.

set priorities, allocate resources, and guide corrective actions.[16] According to OMB guidance, evidence may consist of quantitative or qualitative information and be derived from a variety of sources, including descriptive statistics, performance measurement, policy analysis, program evaluations, or other research.

To ensure that decision makers have the evidence they need, agencies undertake a range of activities. Evidence-building activities involve assessing existing evidence and identifying any need for additional evidence; determining which new evidence to generate, and when and how (such as prioritizing new evidence); and using evidence in decision-making. According to OMB guidance, the strongest evidence generally comes from a portfolio of credible, high-quality sources of evidence to support decision-making.[17]

State Proposed Establishing a New Cyber Diplomacy Bureau, but Did Not Demonstrate That It Used Data and Evidence to Develop the Proposal

State Developed a Proposal to Establish a New Bureau of Cyberspace Security and Emerging Technologies

In June 2019, State notified Congress of its intent to establish the new CSET bureau that would report to the Under Secretary for Arms Control and International Security. Under State's proposal, a Coordinator and Ambassador-at-Large would lead the new bureau, which would merge staff from S/CCI and the Office of Emerging Security Challenges within the Bureau of Arms Control, Verification, and Compliance.[18] The bureau would have a staffing level of 80 full-time employees and a projected budget of $20.8 million.[19] On January 7, 2021, State announced that the Secretary had approved the creation of CSET and directed the department to move forward with establishing the bureau.[20]

According to State's Congressional Notification, the department's rationale for creating the new bureau was to (1) align cyberspace security and emerging technologies security issues with its international security efforts, (2) improve coordination with other agencies working on national security issues, and (3) promote long-term technical capacity within the department. Under this proposal, CSET would not focus on the economic aspects of cyber diplomacy issues. State officials said that, while the department recognized the challenges posed by cyberspace, it considered efforts related to digital economy to be separate and distinct from CSET's cyberspace security focus. However, this separation of responsibilities could complicate the development of consolidated positions on digital economy and cyber policy issues, according to State documentation. Under State's proposal, the Bureau of Economic and Business Affairs

[16]GAO-18-427.

[17]OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, pt. 6, §200.22 (July 2020).

[18]Under H.R. 739, the new office of International Cyberspace Policy would have reported to the Under Secretary for Political Affairs or to an official holding a higher position than the Under Secretary for Political Affairs for a 4-year period. After that 4-year period, the head of the office would have reported to "an appropriate Under Secretary" or an official holding a higher position than Under Secretary.

[19]For fiscal year 2021, State's proposed budget request to establish the new bureau was $17.8 million.

[20]State's announcement noted that CSET would lead U.S. government diplomatic efforts on a wide range of international cyberspace security and emerging technology policy issues that affect U.S. foreign policy and national security, including securing cyberspace and critical technologies, reducing the likelihood of cyber conflict, and prevailing in strategic cyber competition.

would continue to have responsibility for promoting international engagement on internet governance, digital trade, data privacy, and related issues.

In contrast, H.R. 739 would have consolidated State's cyber diplomacy activities, such as those related to international cybersecurity, digital economy, and internet freedom, in a new office. Under this proposed legislation, the head of this office would have served as the principal official for cyberspace policy within State and as the advisor to the Secretary of State for cyberspace issues. In addition, the office would have led State's diplomatic cyberspace efforts, including efforts relating to international cybersecurity, internet access, internet freedom, digital economy, and cybercrime.

State Did Not Demonstrate That It Used Data and Evidence to Develop and Support Its Proposal to Establish CSET

State did not demonstrate that it used data and evidence to develop its plans for CSET. In response to our requests for data and evidence supporting its notification to establish CSET, officials in S/CCI and the Office of the Under Secretary of State for Arms Control and International Security provided briefing slides and an action memo from June 2018 on initial options and the resulting decision for the organizational placement of CSET within State.[21] The briefing slides presented four options for the organizational placement of the new bureau, including fully consolidating cyber and digital policy under a single Under Secretary or separating these issues between different Under Secretaries.[22] These slides also described the "pros" and "cons," or challenges, of each option. For example, the slides noted that the option State ultimately proposed—separating cyber and digital policy between different Under Secretaries—could pose challenges related to coordination and the development of consolidated policy positions.

State officials also provided a subsequent action memo, approved by the Secretary of State, recommending the establishment of CSET in the office of the Under Secretary for Arms Control and International Security and with responsibility for the digital economy retained within the Bureau of Economic and Business Affairs (EB).

However, the proposal for CSET outlined in the memo contained differences from the final proposal as detailed in the 2019 notification to Congress, including differences on which offices State would combine to create the new bureau and on the bureau's overall mission. Further, the memo did not explain how State would address any potential challenges associated with the decision on CSET's organizational placement. For example, the memo did not address how State would coordinate internally on cyber security aspects of digital economy issues, with cyber diplomacy functions split between CSET and EB. The memo also did not specify how State would address the challenge of developing consolidated positions and setting priorities for State's international cyberspace efforts, given the separation of these issues under two different Under Secretaries. Moreover, neither the briefing nor the action memo contained analyses

[21]State officials also provided some related documents, including responses to questions on the 2018 Congressional Notification from House Foreign Affairs Committee staff and a timeline of State's communication with Congressional staff related to CSET.

[22]The options included placing CSET wholly under the Under Secretary for Economic Growth, Energy, and the Environment; under the Under Secretary for Political Affairs; or under the Under Secretary for Arms Control and International Security. A fourth option involved separating cyber and digital policy issues between the Under Secretary for Arms Control and International Security and the Under Secretary for Economic Growth, Energy, and the Environment.

supporting the additional details laid out in the 2019 notification, including support for proposed resource allocations for the new bureau. In addition, the 2018 briefing slides discussed combined lines of effort on cyber diplomacy and cyberspace security and noted that State would conduct a detailed review to more clearly define these efforts and determine their appropriate placement. However, neither the action memo nor the congressional notification discussed this review.

As a result, these documents did not demonstrate that State used data and evidence in developing its notification for establishing CSET. Further, State did not demonstrate that it prepared any other analyses that might provide underlying support for the notification to establish CSET, including State's decision that CSET would focus on the security aspects of international cyber policy and report to the Under Secretary for Arms Control and International Security. State officials noted that they met requirements for notifying Congress on the

proposal.[23] They also noted that they consulted internally with several State bureaus to reach consensus on the details of the proposal. However, State did not provide us documentation from these consultations or with contacts at these bureaus that we could interview to obtain their views.

As noted above, our prior work has shown it is important for agencies to use data and evidence to develop and justify proposed reforms and agency reorganizations.[24] For example, we have reported that agencies are better equipped to address management challenges when program managers effectively use data and evidence, such as program evaluations and performance data, to provide information on how well a program is achieving its goals. Further, when an agency reforms or reorganizes a program, using evidence is critical for setting program priorities, allocating resources, and taking corrective action to improve results. State needs to develop these areas further to better ensure the success of any new organizational arrangement.

Conclusions

The United States faces expanding cyber threats and the challenge of building international consensus on standards for acceptable state behavior in cyberspace. In leading federal efforts to advance U.S. interests in cyberspace, State has notified Congress of its proposal to establish a new bureau focused on cyberspace security and the security aspects of emerging technologies. State, however, has not demonstrated that it used data and evidence to support its proposal, particularly for the bureau's focus and organizational placement. Without developing evidence to support its proposal for the new bureau, State lacks needed assurance that the proposal will effectively set priorities and allocate appropriate resources for the bureau to achieve its intended goals.

[23]Provisions contained in recent annual appropriations measures funding the Department of State, Foreign Operations and Related Programs generally require State to notify Congress at least 15 days before obligating funds to, among other things, create, close, reorganize, downsize, or rename bureaus, centers, or offices. Moreover, State is required to provide Congress a detailed justification containing information specified in explanatory statements accompanying the appropriations measures before undertaking such actions. GAO did not assess whether State complied with these provisions.

[24]GAO-18-427.

Recommendation for Executive Action

The Secretary of State should ensure that State uses data and evidence to justify its current proposal, or any new proposal, to establish the Bureau of Cyberspace Security and Emerging Technologies to enable the bureau to effectively set priorities and allocate resources to achieve its goals.

Agency Comments and our Evaluation

We provided a draft of this report to State for review and comment. We received written comments from State, which are reprinted in the enclosure.

While State disagreed with our characterization of its use of data and evidence to develop its proposal for CSET, it agreed that reviewing such information to evaluate program effectiveness can be useful. State commented that it provided us with what it determined to be appropriate material on its decision to establish CSET and our report noted only the potential coordination challenges resulting from separating cyber and digital policy. State also noted that S/CCI has reported informally to the Under Secretary for Arms Control and International Security since mid-2018 and has not experienced challenges in coordinating cyberspace security policy across the department. State concluded that this experience provides assurance that its proposal to establish CSET will allow the new bureau to effectively set priorities and allocate appropriate resources.[25]

The documents State provided in response to our requests for information supporting its notification to establish CSET—a set of briefing slides and an action memo for the Secretary—did not sufficiently demonstrate that it used data and evidence in developing its proposal. The briefing slides presented four options for the organizational placement of the new bureau, with "pros" and "cons" listed for each option. We focused on the option to place CSET under the Under Secretary for Arms Control and International Security, with responsibility for digital economy issues retained in EB, because that option most closely aligned with the proposal the Secretary of State ultimately approved. State identified three challenges associated with this option: (1) it did not result in clean alignment under one bureau; (2) it could lead to challenges coordinating on economic-related digital policy issues with cyber components; and (3) it could complicate the development of consolidated positions, with two principles covering digital economic issues and security-related cyber issues. Neither the memo nor the notification discussed how the department would specifically address these challenges.

State's comment that S/CCI has experienced no coordination challenges since it began informally reporting to the Under Secretary for Arms Control and International Security in mid-2018 is not evidence that the potential for such challenges—as noted in its June 2018 briefing slides—does not exist. In addition, we were not able to corroborate with other State bureaus that they have not experienced coordination challenges with S/CCI.

For these reasons, we reaffirm our recommendation that State should use data and evidence to justify its current proposal, or any new proposal, to establish CSET. We continue to believe that, without evidence to support the creation of the new bureau, State lacks needed assurance that the bureau will effectively set priorities and allocate appropriate resources to achieve its intended goals.

[25]State's comments do not mention the Secretary's approval of the creation of CSET on January 7, 2021.

- - - - -

We are sending copies of this report to the appropriate congressional committees, the Secretary of State, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact us at (202) 512-5130 or MazanecB@gao.gov, or Nick Marinos on (202) 512-9342 or MarinosN@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report were Rob Ball (Assistant Director), Jeremy Latimer (Analyst-in-Charge), Hoyt Lacy, Umesh Thakkar, Neil Doherty, and Aldo Salerno. Other significant contributors include Mark Dowling, Mary Moutsos, and Benjamin Licht.

Brian M. Mazanec
Director, International Affairs and Trade

Nick Marinos
Director, Information Technology and Cybersecurity

Enclosure

Enclosure: Comments from the Department of State

United States Department of State
Comptroller
Washington, DC 20520

JAN 13 2021

Thomas Melito
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Mr. Melito:

We appreciate the opportunity to review your draft report, "CYBER DIPLOMACY: State Did Not Demonstrate that It Used Data and Evidence to Develop Its Proposal for a New Cyber Diplomacy Bureau" GAO Job Code 104594.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

Sincerely,

Jeffrey C. Mounts

Enclosure:
As stated

cc: GAO – Brian Mazanec
T – Hailey Robbins
OIG - Norman Brown

Department of State Comments on GAO Draft Report

CYBER DIPLOMACY: State Did Not Demonstrate that It Used Data and Evidence to Develop Its Proposal for a New Cyber Diplomacy Bureau
(GAO-21-266RSU, GAO Code 104594)

The Department of State appreciates the opportunity to comment on GAO's proposed report *"Cyber Diplomacy: State Did Not Demonstrate that It Used Data and Evidence to Develop Its Proposal for a New Cyber Diplomacy Bureau"*.

As part of responding to its tasking from the Chairman and Ranking Member of the House Committee on Foreign Affairs to "review State's efforts to advance U.S. interests in cyberspace", the GAO examined the extent to which State used data and evidence to develop and justify its proposal to establish CSET. To address this objective, the draft report states that GAO staff interviewed State officials and reviewed documentation on its planning process for establishing the new bureau. The report states that GAO assessed State's documentation against GAO's key practice, as determined by GAO in its June 2018 report on government reorganization, of "using data and evidence in the development of proposed agency reforms". The report further states that to address this practice, GAO analyzed State's activities leading to the development of the June 2019 Congressional Notification on its proposal for establishing CSET.

The draft report notes that State "did not demonstrate that it used data and evidence" to develop its proposal to establish CSET. The Department of State notes that, based on past practice, it provided GAO investigators with what it determined to be appropriate material concerning the decision to create CSET. The material provided outlines several options the Department considered for creating a new cyberspace security-oriented bureau. The draft report does not examine these options in any detail but rather focuses on the option chosen to create CSET. The draft report notes only that one potential downside identified during the decision process was that separating cyber and digital policy between different Under Secretaries could pose challenges related to coordination and the development of consolidated policy positions.

The Department notes that the Office of the Cyber Coordinator, which has been responsible for cyberspace security diplomacy since 2011, has reported informally to the Under Secretary for Arms Control and International Security since mid-2018, and has experienced no such challenges in coordinating cyberspace security policy development or implementation across the Department. Since mid-2018, the Office of the Cyber Coordinator has continued to successfully develop,

coordinate and implement bilateral and multilateral cyberspace security initiatives, and to support as needed the cyber-related work led by other parts of the Department, including the Bureau of Economic and Business Affairs, and the Bureau of Democracy, Human Rights and Labor. This fact provides support and assurance that the Department's proposal to establish CSET, as notified to Congress in June 2019, will allow it to effectively set priorities and allocate appropriate resources for the bureau to achieve its intended goals.

While the Department disagrees with the GAO characterization of this issue, it does agree that reviewing relevant data and evidence, when available, to evaluate how effectively programs perform can be useful.

Text of Enclosure: Comments from the Department of State

Page 1

Thomas Melito Managing Director

International Affairs and Trade

Government Accountability Office

441 G Street, N.W.

Washington, D.C. 20548-0001

Dear Mr. Melito:

United States Department of State

Comptroller

Washington, DC 20520

We appreciate the opportunity to review your draft report,

"CYBER DIPLOMACY: State Did Not Demonstrate that It Used Data and Evidence to Develop Its Proposal for a New Cyber Diplomacy Bureau" GAO Job Code 104594.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

Sincerely,

Jeffrey C. Mounts

Enclosure:

As stated

cc: GAO - Brian Mazanec T - Hailey Robbins OIG - Norman Brown

Page 2

Department of State Comments on GAO Draft Report

CYBER DIPLOMACY: State Did Not Demonstrate that It Used Data and Evidence to Develop Its Proposal for a New Cyber Diplomacy Bureau (GAO-21-266RSU, GAO Code 104594)

The Department of State appreciates the opportunity to comment on GAO's proposed report "Cyber Diplomacy: State Did Not Demonstrate that It Used Data and Evidence to Develop Its Proposal for a New Cyber Diplomacy Bureau".

As part of responding to its tasking from the Chairman and Ranking Member of the House Committee on Foreign Affairs to "review State's efforts to advance U.S. interests in cyberspace", the GAO examined the extent to which State used data and evidence to develop and justify its

proposal to establish CSET. To address this objective, the draft report states that GAO staff interviewed State officials and reviewed documentation on its planning process for establishing the new bureau.

The report states that GAO assessed State's documentation against GAO's key practice, as determined by GAO in its June 2018 report on government reorganization, of "using data and evidence in the development of proposed agency reforms". The report further states that to address this practice, GAO analyzed

State's activities leading to the development of the June 2019 Congressional Notification on its proposal for establishing CSET.

The draft report notes that State "did not demonstrate that it used data and evidence" to develop its proposal to establish CSET. The Department of State notes that, based on past practice, it provided GAO investigators with what it determined to be appropriate material concerning the decision to create CSET. The material provided outlines several options the Department considered for creating a new cyberspace security-oriented bureau. The draft report does not examine these options in any detail but rather focuses on the option chosen to create CSET. The draft report notes only that one potential downside identified during the decision process was that separating cyber and digital policy between different Under Secretaries could pose challenges related to coordination and the development of consolidated policy positions.

The Department notes that the Office of the Cyber Coordinator, which has been responsible for cyberspace security diplomacy since 2011, has reported informally to the Under Secretary for Arms Control and International Security since mid- 2018, and has experienced no such challenges in coordinating cyberspace security policy development or implementation across the Department. Since mid-2018, the Office of the Cyber Coordinator has continued to successfully develop,

Page 3

coordinate and implement bilateral and multilateral cyberspace security initiatives, and to support as needed the cyber-related work led by other parts of the Department, including the Bureau of Economic and Business Affairs, and the Bureau of Democracy, Human Rights and Labor. This fact provides support and assurance that the Department's proposal to establish CSET, as notified to Congress in June 2019, will allow it to effectively set priorities and allocate appropriate resources for the bureau to achieve its intended goals.

While the Department disagrees with the GAO characterization of this issue, it does agree that reviewing relevant data and evidence, when available, to evaluate how effectively programs perform can be useful.

(Jobcode104594)